JOURNAL OF NUMBER THEORY 67, 170–181 (1997)
ARTICLE NO. NT972176

Rational Points on Algebraic Curves That Change Genus

Sangtae Jeong

Department of Mathematics, University of Texas, Austin, Texas 78712

Communicated by D. Goss

Received October 23, 1996

Let K be an algebraic function field in one variable over an algebraically closed field of positive characteristic p. We give an explicit upper bound for the number

points. We thus prove that every algebraic curve over K that admits genus change under base-field extensions has finitely many K-rational points. © 1997 Academic Press

1. INTRODUCTION

Throughout the paper, unless otherwise specified, let K be an algebraic function field in one variable over an algebraically closed field k of characteristic $p>0$. In other words, K is a function field of a non-singular curve X of genus g defined over k. Let C be an algebraic curve defined over K.

The genus of a curve C relative to K can be defined as the integer g_K such that the Riemann–Roch formula holds; that is, for any K-divisor D of C of sufficiently large degree $\deg(D)$, the dimension $l(D)$ of the K-vector space $L(D)$ of functions of $K(C)$ whose polar divisor is bounded by D is $\deg(D)+1-g_K$. We can also define the absolute genus of C, denoted by $\bar{g}$, to be the genus of C relative to the algebraic closure $\bar{K}$ of a base field K. We then note the inequality $\bar{g}\leqslant g_K$, as the relative genus g_K of C does not change under separable extensions of a base field K, but may decrease under inseparable extensions of K (see [2] and [9]).

An algebraic curve C/K is defined to be non-conservative (or genus-changing) if its relative genus g_K is different from the absolute genus $\bar{g}$. Otherwise, C is said to be conservative. Typical examples of non-conservative curves are given by the equation $x-ax^p=y^p$ $(a\notin K^p,\ p\geqslant 3)$ with relative genus $(p-1)(p-2)/2$ and absolute genus 0, and the equation $y^2=x^p+a$ $(a\notin K^p,\ p\geqslant 3)$ with relative genus $(p-1)/2$ and absolute genus

0022-314X/97 $25.00

0. Note that if a is a pth power in K, then the two equations are rational curves on K, hence they are no longer genus-changing curves. Thus we will assume in what follows that the a appearing in the two equations is not in K^p.

Samuel [5, Chap. III, Theorem 1 and App. 2] proved the following fact: Let K be the same as above, and let C be an algebraic curve of absolute genus $\bar{g} \geqslant 2$ defined over K. If g_K is strictly greater than $\bar{g}$, i.e., C is genus-changing, then the set $C(K)$ of K-rational points of C is finite.

Now the question arises of whether this fact still holds for the curves of absolute genus $\bar{g} = 0$ or 1. For the case where the constant field of the function field K is a finite field, this was proved by Voloch [10]. Fortunately we can easily observe that what he showed for the case $\bar{g} = 1$ also works when we extend a finite field to any algebraically closed field as a constant field of the function field K. On the other hand, for the case $\bar{g} = 0$, Voloch's argument does not work over an algebraically closed constant field of K, because he used the fact that the cardinality of $L(D)$ in the Riemann–Rock formula is finite, i.e., it is a finite-dimensional vector space over a finite constant field of K.

The aim of this paper is to prove that every genus-changing curve of absolute genus 0 defined over K has a finite number of rational points. To do that, we first try to show that the two curves given above as examples of non-conservative curves have a finite upper bound for the number of rational points, and then that every algebraic curve over K of the form $y^p = r(x)$ that admits genus change has at most finitely many K-rational points (Theorem 4). Finally, from this we deduce that every genus-changing algebraic curve over K has a finite number of rational points (Theorem 6).

2. FINITENESS OF RATIONAL POINTS IN SPECIAL CASES

Recall that K is an algebraic function field in one variable over an algebraically closed field k of characteristic $p > 0$. That is, K is a function field of a non-singular curve X of genus g defined over k. We denote by M_K the set of places (by which we always mean here discrete valuations) of K/k and we normalize $v \in M_K$ such that $v(K^*) = \mathbb{Z}$. We may assume that a place $v \in M_K$ is identified with a point on the curve X.

The height of an element $f \in K$ is defined to be the degree of the associated map from $X \to \mathbb{P}^1$, $h(f) = \deg(f: X \to \mathbb{P}^1)$. Hence, we can also set

$$h(f) = \deg(f) = \sum_{v \in M_K} \max\{v(f), 0\} = \sum_{v \in M_K} \max\{-v(f), 0\}.$$

For details on the height, the reader may consult [7, Chap. III]. From this we observe that the number of the set of zeros or poles of $f \in K$ is bounded by $h(f)$. In other words, $\#\{v \in M_K : v(f) > 0\} = \#\{v \in M_K : v(f) < 0\} \leqslant h(f)$.

In order to prove that every algebraic curve over K of absolute genus 0 that admits genus change under extensions of a base field has a finite number of rational points on the curve, we need the following crucial proposition, which is the characteristic p-analogue of an assertion (see Lemma 2.3.2. III in [7]) necessary to prove the weak Mordell–Weil theorem for elliptic curves defined over function fields in one variable over an algebraically closed field of characteristic 0.

PROPOSITION 1. *Let $K = k(X)$ be a function field of a non-singular curve X of genus g defined over an algebraically closed field k of positive characteristic p, let S be a finite subset of the set of all places M_K defined on K, and let $m \geqslant 1$ be an integer. Then the group, $K(S, m) = \{f \in K^*/K^{*m} : v(f) \equiv 0 \pmod{m}$ for all places $v \notin S\}$ is a finite subgroup of K^*/K^{*m}. In the case $m = p$, we have $\#K(S, p) \leqslant p^{s+g}$, where $s = \#S$.*

Proof. Let $s = \#S$, then we have the following exact sequence:

$$1 \to K(\varnothing, m) \to K(S, m) \to (\mathbb{Z}/m\mathbb{Z})^s$$

$$f \mapsto (v(f) \bmod m)_{v \in S}.$$

It thus suffices to prove that $K(\varnothing, m) = \{f \in K^*/K^{*m} : v(f) \equiv 0 \pmod{m}$ for all places v on $K\}$ is finite.

Consider a map $K(\varnothing, m) \to \mathrm{Pic}(X)[m]$, $f \pmod{K^{*m}} \mapsto \mathrm{class}(D_f)$, where $\mathrm{div}(f) = mD_f$ for some divisor $D_f \in \mathrm{Div}(X)$, and $\mathrm{Pic}(X)[m]$ denotes the m-torsion subgroup of $\mathrm{Pic}(X)$.

It is easy to check that this is a well-defined homomorphism. Now suppose that $f \pmod{K^{*m}}$ is in the kernel of this homomorphism. This means that D_f is principal, i.e., $D_f = \mathrm{div}(h)$ for some function $h \in K^*$. Hence, we have

$$\mathrm{div}(fh^{-m}) = \mathrm{div}(f) - m\,\mathrm{div}(h) = \mathrm{div}(f) - mD_f = 0.$$

Thus the function fh^{-m} has no zeros or poles, so it must be constant in k (see Prop. 3.1 II [6]). Since k is algebraically closed, we obtain $f \equiv 1 \pmod{K^{*m}}$. The homomorphism is therefore injective. Finally, we use the fact that $\mathrm{Pic}(X)[m]$ is finite (see p. 64 [4]) to conclude that $K(\varnothing, m)$ is finite.

For the second part, it is easy to see from the exact sequence above that $\sharp K(S, p) \leqslant p^s \sharp K(\varnothing, p)$. The injectivity from the two groups gives $\sharp K(\varnothing, p) \leqslant \sharp \mathrm{Pic}(X)[p]$. We use the well-known fact that the p-torsion subgroup of $\mathrm{Pic}(X)$ has at most p^g elements (see p. 64 of [4]) to show the desired inequality. ▮

Consider a curve C/K defined by $x - ax^p = y^p$, then $\delta = d/da$ is a well-defined non-zero derivation on K/k (remember that $a \notin K^p$). Notice that $(0, 0)$ is an element of the set $C(K)$ of K-rational points on the curve C, so $C(K) \backslash \{(0, 0)\}$ is denoted by $C(K)^*$. We now can give the upper bound for the number of $C(K)$ in the following theorem.

THEOREM 1. $\sharp C(K) \leqslant 1 + (p-1)\, \sharp K(S, p) \leqslant 1 + (p-1)\, p^{\sharp S + g}$, *where* $S = \{v \in M_K : v(a) \neq 0$ *or* $v(da) \neq 0\}$. *Moreover,* $\sharp S \leqslant 6h(a) + 2g - 2$.

Proof. It is easy to see from the construction of S that S is a finite set of places on K.

Define a map $C(K)^* \to K(S, p)$ given by $(x, y) \mapsto xK^{*p}$. First, we need to check that this map is well-defined, i.e., $v(x) \equiv 0 \pmod p$ for all places v outside of S. Let v be a place not in S, then it is easy to show that $v(x) \equiv 0 \pmod p$ if $v(x) \geqslant 0$. If x has a pole at v, i.e., $v(x) < 0$, then we can take the derivation δ of the equation to obtain $\delta x = x^p$. Taking the valuation leads to $pv(x) = v(\delta x) \geqslant v(x) - 1$. Hence, $v(x) \geqslant -1/(p-1) \geqslant -1/2$. This contradicts the fact that v is an integer-valued function on K, and thus implies that the map is well-defined.

It remains to show that the given map is a $(p-1)$-to-1 map. We will show that the inverse image of each $xK^{*p} \in K(S, p)$ has $(p-1)$ elements in $C(K)^*$. Suppose that two rational points (x_1, y_1), (x_2, y_2) in $C(K)^*$ have the same image under this map, i.e., $x_1 K^{*p} = x_2 K^{*p}$. Then, we have $x_1/x_2 = u^p \in K^{*p}$ for some $u \in K^*$. Substituting $ax_i^p + y_i^p$ for each x_i, $i = 1, 2$ and rearranging the terms give the equation

$$a(x_1 - ux_2)^p = (-y_1 + uy_2)^p.$$

Under the assumption that $a \notin K^p$, the coefficient $(x_1 - ux_2)^p$ of a must be 0, hence we have $(x_1, y_1) = (ux_2, uy_2)$ for some $u \in K^*$. Moreover, it is easy to see from this that the relation gives the argument $u = x_1/x_2 = u^p \in K^*$. We thus notice that u is a non-zero element in the prime subfield of K. Since the defining map is not surjective, we get the desired result for the first inequality. The second inequality comes from Proposition 1.

Finally, we can use the height to bound the number of elements in $S = \{v \in M_K : v(a) \neq 0$ or $v(da) \neq 0\}$. It follows from the definition of the height that $\sharp\{v \in M_K : v(a) \neq 0\} \leqslant 2h(a)$. We use the fact that the degree of a canonical divisor (da) is $2g - 2$ to bound the number of the set $\{v \in M_K : v(da) \neq 0\}$ as follows.

$$\begin{aligned}
\#\{v \in M_K : v(da) \neq 0\} &\leqslant \sum_{v \in M_K} |v(da)| \\
&= \sum_{v \in M_K :\, v(da) > 0} |v(da)| + \sum_{v \in M_K :\, v(da) < 0} |v(da)| \\
&= 2g - 2 + 2 \sum_{v \in M_K :\, v(da) < 0} |v(da)| \\
&= 2g - 2 + 2 \sum_{v \in M_K :\, v(da) < 0} -v(da) \\
&\leqslant 2g - 2 + 2 \sum_{v \in M_K :\, v(da) < 0} (-v(a) + 1) \\
&\leqslant 2g - 2 + 2 \sum_{v \in M_K :\, v(a) < 0} (-v(a) + 1) \\
&= 2g - 2 + 2 \sum_{v \in M_K :\, v(a) < 0} -v(a) \\
&\quad + 2\#\{v \in M_K : v(a) < 0\} \\
&\leqslant 2g - 2 + 4h(a).
\end{aligned}$$

Hence we have $\#S \leqslant 6h(a) + 2g - 2$. ∎

Remark 1. For $p > 2$ a prime and $q = p^n$, consider the curve $C_n/\mathbb{F}_p(t)$ defined by

$$x - (t + t^{q+2} + t^{2q+3} + \cdots + t^{(p-2)q+p-1})\, x^p = y^p.$$

It is shown in [1] that $\#C_n(\mathbb{F}_p(t)) \geqslant p^{2n/2n}$ and $\#C_n(\mathbb{F}_{p^{2n}}(t)) \geqslant p^{2n}$. But we can use Theorem 1 to show that $\#C_n(\mathbb{F}_{p^{2n}}(t)) \leqslant \#(C_n(\overline{\mathbb{F}_p}(t))) \leqslant 1 + (p-1)\, p^{(2(p-2)q+2p-3)}$, because any non-constant element in $\mathbb{F}_p(t)$ has as many zeros as its degree over the algebraic closure of $\mathbb{F}_p$. We notice from these that different choices of a in the equation $x - ax^p = y^p$ determine curves that can have arbitrarily many rational points.

COROLLARY 1. *Let $K = \overline{\mathbb{F}_q}(t)$ be the function field of a projective line $\mathbb{P}^1$ over the algebraic closure of a finite field $\mathbb{F}_q$ of characteristic $p \geqslant 3$. Then $(0, 0)$ is the only rational point of the curve C/K: $x - ax^p = y^p$ for infinitely many $a \notin K^p$.*

Proof. For $a = t$, we notice that t has only a zero place v_0 and an infinite place v_∞ on K. So, the set S satisfying the condition in Theorem 1 consists only of two places v_0 and v_∞. For x a non-zero element such that

(x, y) is a rational point of the curve C, then $v(x) \equiv 0 \pmod{p}$ for all places $v \notin S$. From the sum formula of places, we obtain

$$v_0(x) + v_\infty(x) \equiv 0 \pmod{p}.$$

For $r = v_0(x) \in \mathbb{Z}$, then we can show that $v(t^{-r}x) \equiv 0 \pmod{p}$ for all places v on K. This means that the function $t^{-r}x$ is in $K(\varnothing, p)$, where $K(\varnothing, p)$ is as in Proposition 1.

Now we want to claim that $x = tu^p$ for some $u \in K^*$. It is easy from Proposition 1 to see that $\sharp K(\varnothing, p) = 1$, because $\mathbb{P}^1$ has genus 0. This implies that we can write $x = t^r u^p$ for some $u \in K^*$. Here we can assume, if necessary, that $0 \leqslant r \leqslant p-1$. When we substitute $x = t^r u^p$ into the equation of C and take the derivation $\delta = d/dt$, we obtain $rt^{r-1}u^p - (t^r u^p)^p = 0$. Thus, taking a valuation in the preceding equation gives $r - 1 \equiv 0 \pmod{p}$, so it follows from the assumption on r that $r = 1$.

Finally, after plugging $x = tu^p$ into the equation once again, taking the derivation of the equation gives $1 = tu^{p-1}$. From this it follows that x does not satisfy the equation since there is no element $u \in K^*$ satisfying $tu^{p-1} = 1$. From the discussion above we conclude that $(0, 0)$ is the only rational point on the curve. The same argument applies to t^m, where m is relatively prime to p. ∎

THEOREM 2. *Consider a curve C/K defined by $y^2 = x^p + a$, then we have $\sharp C(K) \leqslant 2\sharp K(S, p) \leqslant 2p^{\sharp S + g}$, where $S = \{v \in M_K : v(a) \neq 0 \text{ or } v(da) \neq 0\}$.*

Proof. For a given S, define a map $C(K) \to K(S, p)$ given by $(x, y) \mapsto yK^{*p}$. It is easy to check that the map is exactly two-to-one if we follow the same procedure as in the second part of the proof of Theorem 1. It thus suffices to show that the given map is well-defined. Let v be a place outside of S. It is easy to check that $v(y) \equiv 0 \pmod{p}$ if x has a zero or a pole at v. If $v(x) = 0$, then we notice that $v(y) \geqslant 0$, and taking the derivation $\delta = d/da$ of the equation, we have $2y\,\delta y = 1$. Thus taking the valuation gives

$$-v(y) = v(\delta y) \geqslant v(y) - 1,$$

so $v(y) \leqslant \frac{1}{2}$. It follows that $v(y) = 0$ since v is an integer-valued function on K. ∎

COROLLARY 2. *Let $C: y^2 = x^p + a$ be a curve defined over a rational function field $\overline{\mathbb{F}_q}(t)$ over the algebraic closure of a finite field $\mathbb{F}_q$ of positive characteristic p. Then C has no rational points for infinitely many $a \notin K^p$.*

Proof. In the case where characteristic $p = 2$, the given curve has no rational points over any function field for any $a \notin K^2$. It thus suffices to show that the statement holds for characteristic $p \geqslant 3$. For $a = t$ and a

rational point (x, y) of C, we can write $y = t^r u^p$ where $0 \leqslant r \leqslant p-1$ from the same observation as Corollary 1. $2r - 1 \equiv 0 \pmod{p}$ is obtained from the equation $v(y) + v(\delta y) = 0$. The only possible value of r is $(p+1)/2$ from the condition on r. Hence, $y = t^{p+1/2}u^p$ is the y-coordinate for a rational point (x, y). After plugging y in the equation of C, we have

$$x^p = y^2 - t = t^{p+1}u^{2p} - t = t(t^p u^{2p} - 1) = t(tu^2 - 1)^p.$$

Since t is not a pth power in $\overline{\mathbb{F}_q}(t)$, $tu^2 - 1$ should be 0. But one can easily check that no element $u \in \overline{\mathbb{F}_q}(t)$ satisfies $tu^2 = 1$. This means that the curve for $a = t$ has no rational points. Moreover we can apply the same argument to the case where $a = t^{mp+1}$ and m is any even positive integer. ∎

3. GENERALIZATION

In this section we will deal with a genus-changing curve of the form $y^p = r(x) \in K(x)$. First we consider a particular polynomial $r(x)$ of degree n satisfying: $r(0) = 0$, n is relatively prime to p, and $r(x)$ has at least one non-zero term whose degree is strictly less than p. For a finite set S of places on K associated with the coefficients of $r(x)$, we can define a map from the set of non-zero x-coordinates of K-rational points on the curve to $K(S, p)$. As we will see, the fact that the curve is nonconservative implies that the defining map is finite-to-one. We then can give an explicit upper bound for rational points on such a curve. Using a change of variables, we can prove the finiteness of rational points for all genus-changing curves defined by $y^p = r(x) \in K[x]$ for general polynomials $r(x)$. Finally, following Voloch's argument that every genus-changing curve of absolute genus zero over K is a finite cover of a genus-changing curve given by $y^p = r(x) \in K(x)$, we can prove that every genus-changing curve of absolute genus zero over K has a finite number of rational points.

LEMMA 1. *Let* $r(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x \in K(x)$ *be a polynomial of degree* n *such that* $(n, p) = 1$, *and* $c_j \neq 0$ *for some* $j \leqslant p-1$. *Assume* $T = \{a \in K^* : r(a) \in K^p\}$ *is non-empty. Then there is a finite set* S *of places on* K *such that* $v(a) \equiv 0 \pmod{p}$ *for all places* $v \notin S$ *and all* $a \in T$. *Moreover,* $\sharp S \leqslant 2\sum_{i=1}^{n} h(c_i)$.

Proof. Let $r(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x$ be a polynomial of degree n satisfying all the hypotheses, and let $S = \{v \in M_K : v(c_i) \neq 0$ for some $1 \leqslant i \leqslant n\}$. Since S consists of zeros or poles of some coefficients of $r(x)$ it is easy to see from the definition of the height of an element in K that $\sharp S \leqslant 2\sum_{i=1}^{n} h(c_i)$. We thus need to show that $v(a) \equiv 0 \pmod{p}$ for all places $v \notin S$ and $a \in T$.

If v is outside of S and a is in T, then we have $v(c_i) = 0$ for all $1 \leqslant i \leqslant n$, and $r(a) = b^p = c_n a^n + \cdots + c_1 a$ for some $b \in K$. Here we can break up our proof into two parts. First, for $b = 0$, then we know that at least two elements of the equation have the same valuation. This implies that $v(a) = 0$.

Second, for $b \neq 0$, then taking the valuation on both sides, we notice that the left-hand side of the equation is a multiple of p, but the right-hand side depends on the sign of $v(a)$. If $v(a) < 0$, i.e., a has a pole at v, then $pv(b) = v(b^p) = v(c_n a^n + \cdots + c_1 a) = v(c_n a^n) = v(a^n) = nv(a)$. It follows from the hypothesis $(n, p) = 1$ that $v(a) \equiv 0 \pmod{p}$.

If $v(a) > 0$, i.e., a has a zero at v, then $pv(b) = v(b^p) = v(c_n a^n + \cdots + c_1 a^1) = v(c_j a^j) = jv(a)$ for some $1 \leqslant j \leqslant p-1$, from the hypothesis on $r(x)$. The relation $(p, j) = 1$ leads to $v(a) \equiv 0 \pmod{p}$. ∎

LEMMA 2. *Let C be a non-conservative curve over K defined by $y^p = r(x) \in K[x]$. Then there is at least one coefficient of $r(x)$ that is not in K^p.*

Proof. Suppose not. Then we have $r(x^p) = s(x)^p$ for some polynomial $s(x) \in K[x]$. Consider the map from $\mathbb{A}^1$ to C defined by $x \mapsto (x^p, s(x))$. This implies that C is parameterizable, which contradicts the fact that C is non-conservative. ∎

THEOREM 3. *Consider a genus-changing algebraic curve C/K defined by $y^p = r(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x$ such that $(n, p) = 1$, $c_j \neq 0$ for some $j \leqslant p-1$. Then $\sharp C(K) \leqslant 1 + (n-1)\, p^{s+g}$, where $s \leqslant \sum_{i=1}^{n} 2h(c_i)$.*

Proof. Let $C(K)$ be the set of all K-rational points of C satisfying all the conditions on $r(x)$. Let $T = \{a \in K^* : r(a) \in K^p\}$ be the set of non-zero x-coordinates of rational points in $C(K)$ (Here we assume T to be non-empty, otherwise $C(K)$ contains only one rational point $(0, 0)$). Let S be the set of finite places associated with $r(x)$ and T, which is obtained from Lemma 1, and let $K(S, p) = \{f \in K^*/K^{*p} : v(f) \equiv 0 \pmod{p}$ for all $v \notin S\}$ be a finite set corresponding to it.

Now consider a map from T to $K(S, p)$ defined by $a \mapsto aK^{*p}$. It follows from Lemma 1 that this map is well-defined. We will show that it is at most an $(n-1)$-to-one map of sets.

Suppose that two elements $a_1, a_2 \in T$ have the same image under this map, i.e., $a_1 K^{*p} = a_2 K^{*p}$. Then we have $a_1 = a_2 u^p$ for some $u \in K^*$, and for the polynomial $r(x)$ we get the following:

$$\begin{aligned} r(a_1) &= r(a_2 u^p) \\ &= c_n (a_2 u^p)^n + \cdots + c_1 (a_2 u^p) \\ &= (c_n a_2^n)\, u^{pn} + \cdots + (c_1 a_2)\, u^p \in K^p. \end{aligned}$$

Taking the derivation δ of the last equation gives

$$0 = \delta(c_n a_2^n)\, u^{pn} + \cdots + \delta(c_1 a_2)\, u^p.$$

Here we can consider the right-hand side of this equation as a polynomial in the variable u^p, say $F(u^p)$. Then we claim that F is a polynomial of degree at most n and is not identically zero. This will imply that the map defined above is at most $(n-1)$-to-one. From this we will be able to deduce that the set T consisting of non-zero x-coordinates of rational points of the curve C has at most $(n-1)\,\sharp K(S, p)$ elements. Hence $\sharp C(K) = \sharp T + 1 \leqslant 1 + (n-1)\,\sharp K(S, p) \leqslant 1 + (n-1)\, p^{\sharp S + g}$. We observe that 1 is a contribution to a rational point $(0, 0)$.

Let us now prove the claim. Suppose that F is identically zero as a polynomial in the variable u^p. Then we have $\delta(c_i a_2^i) = 0$ for all $1 \leqslant i \leqslant n$. This means that $c_i a_2^i$ is in K^p for each i. Making a change of variables from x to $a_2 x$ on the curve, we reduce the curve to another curve, $y^p = r(a_2 x)$, whose x-coefficients are now all powers of p. But this contradicts Lemma 2. ∎

THEOREM 4. *Every genus changing curve C/K of the form $y^p = r(x) \in K[x]$ has finitely many rational points.*

Proof. Let $\mathscr{S}$ be the collection of all genus-changing curves over K of the form $y^p = r(x)$ with infinitely many rational points. It then suffices to show that $\mathscr{S}$ is an empty set. Suppose that $\mathscr{S}$ is not empty. Choose a curve $C \in \mathscr{S}$ such that C has minimal degree n in x. By a change of variables, if necessary, we may assume that $r(0) = 0$, i.e., $r(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x$. Let j be the smallest index for which $a_j \neq 0$. We then notice that $j \geqslant 1$, and we can write $j = pl + q$ for some $l \geqslant 0$ and $0 \leqslant q \leqslant p-1$. We here consider two cases for l. Suppose that $l \neq 0$. Then we can construct the polynomial $r_1(x) = x^{-pl} r(x)$, which has degree strictly less than that of $r(x)$. We also note that the curve defined by $y^p = r_1(x)$ is birational equivalent to the chosen curve C, hence it is also a genus-changing curve whose rational points are different from those of C by only finitely many points. Hence it contradicts the minimality of degree of $r(x)$.

Suppose now that $l = 0$. Then q is not equal to zero. If the degree n of $r(x)$ is relatively prime to p, we can use Theorem 3 to show that this curve has finitely many rational points. This contradicts that the number of rational points on C is infinite. Thus, $p \mid n$, and we can construct $r_2(x) = x^n r(1/x)$, which is of degree $< n$. It now is not hard to check that the curve defined by $y^p = r_2(x)$ is birational equivalent to the curve C. Hence the same argument as above leads to contradiction of minimality on degree. ∎

THEOREM 5. *For $p>2$ a prime, consider an algebraic curve C/K defined by*

$$y^p = r(x) = a_0 x + a_1 x^{e_1} + a_2 x^{e_2} + \cdots + a_{d-1} x^{e_{d-1}} + a_d x^{e_d},$$

where all e_i are multiples of p. Then C is genus-changing if and only if $a_j \notin K^p$ for some $j \geqslant 1$.

Proof. Assume that $a_i \in K^p$ for all $i \geqslant 1$. Then it follows from Lemma 1 that $a_0 \notin K^p$. Taking the derivation δ of the equation gives

$$\begin{aligned} 0 = \delta(y^p) = \delta(r(x)) &= r'(x)\,\delta x + r^{\delta}(x) \qquad (*) \\ &= a_0(\delta x) + (\delta a_0)\,x \\ &= \delta(a_0 x). \end{aligned}$$

This implies that $a_0 x \in K^p$. Hence we can show that the given curve is parameterizable, which contradicts that C is genus-changing.

For the converse, assume that C is conservative. Then we note that C has absolute genus 0, which implies that C is parameterizable. Hence there exist two rational functions $x = \varphi(t)$, $y = \phi(t)$, of which at least one is not constant, satisfying the equation of C. Viewing x as a transcendental element over K we can select δx arbitrarily. By setting $\delta x = 0$ we obtain $r^{\delta}(x) = \delta a_0 x + \delta a_1 x^{e_1} + \cdots + \delta a_d x^{e_d} = 0$ from the equation in $(*)$. It follows then from the hypothesis that the preceding equation is a polynomial of degree non-zero multiple of p. Since this polynomial has finitely many roots in K, then x must be constant, viewed as a function of infinitely many values of t. Thus, in a similar way, y is also constant. ∎

Remark 2. For $p>2$ a prime and $q = p^l$, let $\Phi(t) = a_0 F^0 + a_1 F + \cdots + a_d F^d$ be a t-module of dimension 1 defined over $\mathbb{F}_q(T)$ such that a_j is not a pth power in $\mathbb{F}_q(T)$ for some $j \geqslant 1$, where F is the Frobenius map relative to $\mathbb{F}_q$. Consider the equation (Φ, q): $Y^{q^d} \Phi(t)(X/Y) = Z^p$; which is the inhomogeneous analogue of the Fermat curve over a rational function field $\mathbb{F}_q(T)$. Denis [3] uses the canonical height to prove that this equation (Φ, q) has at most finitely many rational solutions if $(X, Y) = 1$. The equation also reduces to a genus-changing algebraic curve given by

$$y^p = r(x) = a_0 x + a_1 x^q + a_2 x^{q^2} + \cdots + a_{d-1} x^{q^{d-1}} + a_d x^{q^d},$$

we then use Theorem 4 to show that the curve has a finite number of rational points.

LEMMA 3. *Let C/K be a genus-changing curve defined by $y^p = r_1(x)/r_2(x) \in K(x)$, then the number of the set $C(K)$ of rational points on C is at most finite.*

Proof. By multiplying a pth power of a denominator $r_2(x)$ on both sides of the equation of C, we have $(yr_2(x))^p = r_1(x)\, r_2^{p-1}(x)$. The preceding equation gives an algebraic curve C' defined by $v^p = r(u)$ where $r(u) = r_1(u)\, r_2^{p-1}(u) \in K[u]$. Now it is easy to show that two curves C and C' are birational equivalent, hence C' is also a genus-changing curve. It follows immediately from Theorem 4 that the cardinality of $C'(K)$ is at most finite. We also note that two sets $C(K)$ and $C'(K)$ differ by only a finite number of elements, which are contributed by zeros of $r_2(x)$. The above discussion concludes that the number of $C(K)$ is finite. ∎

THEOREM 6. *Let K be a function field in one variable over an algebraically closed field of positive characteristic p. Then every non-conservative algebraic curve C over K has finitely many K-rational points.*

Proof. Let C_n/K, $n = 0, 1, 2, \ldots$, be the algebraic curve whose function field is the field $K \cdot (K(C))^{p^n} = K(C_n)$, and let g_n be the genus of C_n. Then the sequence g_n is non-increasing because the corresponding function field is increasing purely inseparably. The absolute genus $\bar{g}$ of C is obtained as the constant value of g_n for all n sufficiently large (see [8]). Samuel proved the theorem for the case of $\bar{g} \geqslant 2$ in [5]. For the elliptic case of $\bar{g} = 1$ the theorem was proved by Voloch [10, Theorems 2 and 4]. (Note that his proof works when the constant field of a function field is extended from a finite field to its algebraic closure.)

Here we consider the rational case of $\bar{g} = 0$. Let n be such that $g_{n-1} > g_n = \bar{g}$. Let $y \in K(C_{n-1}) \backslash K(C_n)$, then $r = y^p \in K(C_n)$ and $K(C_{n-1}) = K(C_n)(y)$. This means that the cover of C_n defined by the equation $y^p = r$ is exactly the curve C_{n-1}. Notice that the curve C_{n-1} is, by construction, non-conservative, and that $K(C_n)$ is a rational function field since $g_n = 0$. Hence the given r is a rational function of one variable x in $K(C_n)$. Now it is easy to see from Lemma 3 that the set $C_{n-1}(K)$ of rational points of C_{n-1} is finite. It follows by p-extension field of function fields that $C_{n-1}(K), \ldots, C_0(K) = C(K)$ are all finite. ∎

ACKNOWLEDGMENTS

I thank my advisor, J. F. Voloch, for encouraging me with many helpful discussions. I also thank the referee for a useful suggestion on how to simplify the proof of Theorem 4.

REFERENCES

1. D. Abramovich and J. F. Voloch, Lang's conjectures, fibered powers, and uniformity, *New York J. Math.* **2** (1996), 20–34.
2. E. Artin, "Algebraic Numbers and Algebraic Functions," Gorden and Breach, New York/London/Paris, 1967.
3. L. Denis, Le Théorème de Fermat-Goss, *Trans. Amer. Soc.* **343** (1994), 713–726.
4. D. Mumford, "Abelian Varieties," Oxford Univ. Press, Bombay, 1970.
5. P. Samuel, Lectures on old and new results on algebraic curves, Tata Institute of Fundamental Research, Bombay, 1966.
6. J. H. Silverman, "The Arithmetic of Elliptic Curves," Springer-Verlag, New York, 1986.
7. J. H. Silverman, "Advanced Topics in the Arithmetic of Elliptic Curves," Springer-Verlag, New York, 1994.
8. H. Stichtenoth, Zur Konservativität algebraischer Funktionenkörper, *Crelle* **301** (1978), 30–45.
9. J. T. Tate, Genus change in inseparable extensions of function fields, *Proc. Amer. Math. Soc.* **3** (1952), 400–406.
10. J. F. Voloch, A Diophantine problem on algebraic curves over function fields of positive characteristic, *Bull. Soc. Math. France* **119** (1991), 121–126.